Just Because You're Paranoid, Doesn't Mean They're Not After You

SCRIPT-ed

Volume 3, Issue 4, June 2006

Just because you're paranoid, doesn't mean they're not after you: Legislative developments in relation to the mandatory retention of communications data in the European Union

Judith Rauhofer[*]

Abstract

In the wake of the terrorist attacks in New York, Madrid and London the mandatory retention of communication data by communications service providers has become a contentious issue between the governments of nation states and the communications industry and civil rights campaigners. While the former claim that such retention is necessary for the purpose of national security and the detection and investigation of crime, the latter argue that data retention represents an attack on the rights and freedoms of individuals without evidence that measures will indeed increase the security of citizens. This paper explores the legislative developments, which have taken place in the UK and the European Union in recent years, focusing in particular on the draft Directive on data retention which was adopted in February 2006.

DOI: 10.2966/scrip.030406.322

[*] Senior Lecturer, Liverpool John Moores University, Liverpool.

1. Introduction

It is without a doubt that the advent of information technology and, in particular, the Internet has had an impact on the private life of citizens in developed (and increasingly in developing) countries not seen since the industrial revolution. The "digitalisation" of everyday tasks such as reading the newspaper, listening to music and even shopping for groceries has changed the face of public life to a point where many people now find it difficult to imagine a day without access to a computer. No more is this the case than in the area of communication. Where previous generations managed to sustain personal and business relationships by way of postal letters, today even the smallest disturbance in the telecommunications system has the potential to bring businesses, from high street retailers to blue chip companies, to their knees. In our working practices we have become entirely reliant on e-mail and the WorldWideWeb.

What is less appreciated by many using the new technologies is just how much information about oneself, one's habits and one's personal lives one leaves behind during that online shopping spree, when texting friends or sending a quick e-mail. These footprints of people going about their daily business are known in the IT and communications industry as "communications data". They include a variety of information generated in the context of making telephone calls, sending and receiving e-mails and accessing the Internet.

In the case of e-mail, the data may include the time the e-mail was sent, the addressee and the size of the file. In the case of a telephone call they may include the number called, the number from which the call was made, and the length of the call. An ISP providing access to the Internet will keep a log of the time access was initiated and terminated and, in the case of access to the WorldWideWeb, the URLs of websites visited and the order in which they were accessed. Collectively, such data are known as "traffic data". Communications data also include personal information relating to the identity of the person making the phone call or accessing the Internet such as name, billing address, etc., commonly known as "subscriber data". Finally, where calls are made using a mobile phone call, the mobile phone provider will also be able to establish the location of the caller at the time of the call ("location data").

It is widely held, that "as the technology and business models evolve, communications data will provide a very rich and colourful picture of an individual's interactions, associations, activities, thereabouts, and interests"[1]. This applies, in particular, to traffic data. As Caspar Bowden, then Director of the Foundation for Information Policy Research (FIPR) explains:

> *Traffic data constitutes a near complete map of private life: whom everyone talks to (by e-mail and phone), where everyone goes*

[1] M Farrell, "Communications data retention in the UK" (2001) 3, *E-commerce law & policy,* 11.

> *(mobile phone location co-ordinates), and what everyone reads online (websites browsed).*[2]

In relation to the majority of citizens most people would argue that communications data is strictly private information which should be treated as such. However, it is undeniable that the developments and the increase in the use of information technology have also given rise to an increase in its use for less salubrious purposes. IT opens up new avenues of communication, but it also opens up new avenues of committing crime, both against the individual and against the state.

It is for this reason that communications data have become a contentious issue between those who want to protect the private sphere of individuals by restricting their disclosure to third parties and those who feel that limited disclosure is justifiable for the purpose of promoting certain "public interests". Law enforcement authorities ("LEAs") in particular have argued for some time that they should be permitted to access communications data for the purpose of crime prevention and national security, claiming that access to and the use of communications data has been of significant benefit and value in the investigation of the 9/11 attacks[3]. LEAs also say that the detection and prosecution of many forms of crime would be impossible without access to communications data. Consequently, governments faced a delicate balancing act between succumbing to the demands of civil liberties campaigners for the protection of individuals' privacy from state interference and the claims of their law enforcement communities that without such rights of access they would no longer be able to perform their function in the face of technological advancement.

However, the debate about data retention did not surface – as many observers claim - as a direct consequence of the terrorist attacks on New York, Madrid and London. First moves in this respect date back to a time long before 9/11.

This article will examine the historical developments in relation to the mandatory retention of communications data both in the UK and the European Union. It will analyse the "business case" for data retention and examine alternative ways of combating the use of information technology for criminal and terrorist purposes. It will also provide a critique of how current legislation allows public authorities not involved in law enforcement to access data retained under anti-terrorist laws for purposes unrelated to the aims of crime prevention and prosecution. It will consider the legal basis for mandatory data retention, the provisions contained in the recently adopted Data Retention Directive and the likely consequences of its adoption. It will track the passage of the Directive through the legislative process, focusing in particular on the way in which the EU institutions "co-operated" to achieve political agreement on this very controversial issue. Finally, the paper will aim to provide an appraisal of the need for mandatory data retention in general based on arguments brought forward by the law enforcement community, civil rights campaigners and the communications industry.

---

[2] C Bowden, "Closed circuit television for inside your head: blanket traffic data retention and the emergency anti-terrorism legislation" (2002), *Duke L. & Tech. Rev*., 0005, 6.

[3] So, for instance, Detective Inspector Mike Ford of the National Hi-Tech Crime Unit in a letter to providers who voluntarily preserved communications data on the LEAs' request for a short period after the attacks, see the Report of an Inquiry by the All Party Internet Group on Communications Data at 28.

2. Access to communications data

The term 'communications data' first made its appearance in the UK statute books in s.21 (4) of the Regulation of Investigatory Powers Act 2000 ('RIPA'). Part I of Chapter II RIPA was intended to provide the solution to a problem faced law enforcement agencies ("LEAs") following the coming into force of the Data Protection Act 1998 ("DPA"). Under the second data protection principle set out in Schedule 1 DPA, data controllers, i.e. the person or organisation responsible for determining the purposes for which and the manner in which personal data are processed, must only use communications data for the (business) purpose for which it was originally collected and for no other purpose. In practice, communications data frequently are a by-product of the service provision by communication service providers such as ISP, telephone and mobile telephone providers ("CSPs") or are collected and used for the CSPs' own commercial purposes (e.g. billing). The second principle therefore prevented disclosure of the data to third parties including LEAs.

Sections 28 and 29 DPA contain a number of exemptions from the non-disclosure principle where disclosure is necessary for the purposes of national security, the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty. However, this does not imply an obligation on the part of the CSPs to disclose such data. Rather it grants CSPs an exemption from their strict legal duty to keep the data confidential. The decision whether to disclose the data (and the liability for wrongful disclosure) remained with the CSPs.

Prior to the enactment of RIPA, the LEAs only had a legal right to access to communications data where such access was obtained on the basis of judicial warrants under the Police and Criminal Evidence Act 1984 ('PACE'). Other public authorities could request – and were in many case granted – access under a canon of so called "legacy legislation" which ranked from The Health & Safety at Work etc Act 1974 to the Charities Act 1993[4].

In all other cases LEAs and public authorities had to rely on "section 29(3) requests". As the All Party Internet Group (APIG) points out in its report of its inquiry into communications data, whilst CSPs were willing to grant such requests from LEAs, they were less happy to do so in the case of other public authorities. This was due to the "significant trust in police procedures because of the way that requests were funnelled through specialist departments". This trust "did not extend to public authorities in general"[5] which made it almost impossible for them to obtain access to the communications data retained by CSPs.

Part I of Chapter II RIPA was designed to address this issue by providing a legislative framework covering the requisition, provision and handling of communications data by public authorities. It specifies the duties and responsibilities placed upon each party involved in the process of disclosure and contains a "system of safeguards" which claim to "reflect the requirements of Article 8 of the European Convention on

---

[4] It is outside the scope of this article to consider the issues surrounding the continued existence of legacy legislation after the enactment of RIPA. For a detailed discussion of the relevant points, please see Report of an Inquiry by the All Party Internet Group on Communications Data ("APIG Report"), at 15-16.

[5] APIG Report, at 9.

Human Rights"[6]. Section 22(2) RIPA lists a number of purposes (RIPA purposes) for which persons designated under the Act may obtain access to communications data held by communication service providers. Currently access can be obtained in the interests of national security, for the purpose of preventing or detecting crime or of preventing disorder, in the interests of the economic well-being of the UK, in the interests of public safety, for the purpose of protecting public health, for the purpose of assessing or collecting any tax, duty or levy and for the purpose, in an emergency, of preventing death or of preventing or mitigating injury or damage to a person's physical or mental health.[7] Under section 25(2) RIPA individuals holding certain offices, ranks or positions with relevant public authorities have the right to, and grant authorisation to others within the same public authority to, obtain and disclose communications data. For the purposes of section 22 of the Act, a "public authority" means a body or office which is listed section 25 (1) of the Act[8]. That list may be added to by order of the Secretary of State with the approval of both Houses of Parliament (section 25(4) RIPA)[9].

3. The right to introduce the mandatory retention of communications data

Even more alarming for public authorities (including LEAs) was the fact that, under the fifth data protection principle, CSPs are generally not allowed to retain

---

[6] Explanatory Notes to Regulation of Investigatory Powers Act 2000, para.156

[7] The Home Office has recently proposed a new draft Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006 which adds new purposes to section 22(2) RIPA. Under the new proposals, designated persons may also obtain and disclose communications data to assist investigations into alleged miscarriages of justice, for the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime, or for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for his death or condition. The draft Order, available at <*http://www.opsi.gov.uk/si/si2006/draft/20064600.htm*> is subject to approval by both Houses of Parliament.

[8] This article does not discuss the minutiae of the access procedure, such as the different levels and validity of authorisation, the notice procedure, who exactly within the relevant public authorities would be entitled to request disclosure of communications data and who would be responsible for supervision and oversight of the scheme. These questions are intended to be addressed in a Code of Practice to be prepared and published by the Secretary of State under section 71 RIPA. No final statutory code of practice regarding the acquisition and disclosure of communications data has been published to date. A draft code was the subject of a public consultation in August 2001, but further work on this code was shelved in light of adverse comments on Chapter II of Part I of RIPA in 2001. The government has recently issued a consultation on a revised code of practice which indicates that the original draft code of practice has been refined and developed over the past two years to take account of various matters, including addressing issues of concern to Parliament, such as data protection safeguards. Responses on the consultation are requested by 30 Aug 2006, see Consultation paper and revised Statutory Code for Acquisition and Disclosure of Communications Data, June 2006, available at <*http://www.homeoffice.gov.uk/documents/351628/ripa-part1.pdf?view=Binary*>

[9] With effect from 5 Jan 2005, the Regulation of Investigatory Powers (Communications Data) Order 2003 (SI 2003/3172) (the 2003 Communications Data Order) added a number of public authorities to the list in section 25 (1) of the Act. The draft Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006 recently proposed by the Home Office (see supra, note 7) will add further public authorities and designated persons to that list and remove or update entries.

communications data for longer than is necessary for the purpose for which they were collected. After that the data must be erased. An even more specific obligation to erase or make anonymous all traffic data arising in the course of telecommunications calls was also set out in regulation 6(2) of the Telecommunications (Data Protection and Privacy) Regulations 1999 (SI 1999/2093)("1999 Regulations"), whereby: "[u]pon the termination of the call in question, save as provided in regulations 7(2) and 8(2), such data […] shall be erased or shall be so dealt with that they cease to be such data […]".

For public authorities this meant that access to communications data under RIPA was only possible for the duration that such data were required by CSPs for the CSPs' own business purposes. Depending on the nature of the data, retention was permitted for anything from several months, in the case of billing data, to a few hours, in the case of less commercially sensitive data such as weblogs. The changing nature of the services offered by CSPs also served to limit the collection and retention of data: whilst a certain amount of traffic data was required for billing purposes by an ISP providing a metered access service, the introduction of 'flat-rate' services made the collection of such data unnecessary and therefore unlawful.

Consequently, LEAs argued that legislation was required to ensure that the data they wished to access were not deleted by CSPs – in compliance with CSPs' obligation under the fifth data protection principle and the 1999 Regulations – before such access could be granted. On this basis, it is worth examining the reasons given by LEAs and the various other public authorities for their need to access, and for the CSPs' corresponding obligation to retain, communications data.

3.1. The business case for mandatory data retention

It has been remarked by many opponents of mandatory data retention provisions that no business case has ever been made for the need to retain such large amounts of data on all citizens. One of the earliest efforts by the UK law enforcement community to persuade the government to introduce data retention legislation was made in a submission on communications data retention law by the National Crime and Intelligence Service ('NCIS')[10] which was submitted to the Home Office on 21 August 2000.

Allegedly prepared after consultation with "a number of leading UK Communications Service Providers"[11] the submission contained a variety of recommendations on the general issue of data retention, the type of data to be retained, the retention period and the identity of those responsible for retention[12].

It claimed that data retention and access to retained data was necessary for four main purposes:

---

[10] NCIS submission on data retention law: Looking to the future – clarity on communications data retention law of 21 Aug 2000

[11] Id. at para. 1.1.2

[12] The report does not go into any detail about the providers' reaction to their proposals during the 'consultation'. Instead, it remarks that it would be "inappropriate" to comment on those individual reactions, see para. 1.1.2. In view of the fairly well know opposition by providers' to data retention it is unsurprising that this point was merely touch upon in the NCIS report.

- as primary evidence, e.g. location data could be used to locate the proximity of a mobile phone user to a crime scene;
- as corroborative evidence, e.g. traffic data could serve to establish proof of association between criminal elements through telephone contact;
- for intelligence purposes when identifying and tracing associates and locating places of significance; and
- as post-trial evidence to support appeals against convictions and investigations into miscarriage of justice.[13]

The report made it clear that the LEAs favoured blanket data retention over other forms of data collection because "in the absence of data retention legislation the only means by which the Agencies could lawfully attempt to require providers to retain data that may subsequently be relevant to an investigation, is to obtain a Production Order"[14]. Orders would have to be sought on every occasion that a serious crime had been committed and served on each and every provider. The approach was described as "unworkable and a greater infringement on privacy"[15] than data retention.

The reaction to the proposals by the media, civil liberties organisations and many politicians from all parties was one of unrestrained outrage. Lord Cope, a conservative peer and expert on privacy issues, was quoted to have said that whilst being sympathetic to the need for greater powers to fight modern types of crime "vast banks of information on every member of the public can quickly slip into the world of Big Brother"[16]. Both the FIPR and the human rights organisation Statewatch condemned the proposals and most of the national papers asked for confirmation from the Home Office, the addressee of the submission, that the proposals would not be endorsed.

So big was the stir caused by the leaking of the proposals that Patricia Hewitt, then the so-called 'E-minister', and Charles Clarke, then a junior minister in the Home Office, were forced to write an open letter to the Independent on Sunday on 28 January 2001, in which they made it clear that the Home Office had no plans to act on the proposals[17]. When asked about the matter earlier during a session of the Select Committee on Trade and Industry on 13 December 2000, Hewitt had replied:

> *I do not agree with the proposals. I saw them in the press, I think, ten days ago. I have not had formal communications with the Home Office, I have discussed it informally with Charles Clarke and I understand it is his view as well that that proposal should not be implemented.*[18]

---

[13] Id. at para. 1.2.1

[14] Id. at para 3.1.5

[15] Id. at para. 3.1.5

[16] See The Observer, 3 Dec 2000, "Secret plan to spy on all British phone calls"

[17] P Hewitt and C Clarke, Joint letter to Independent on Sunday, 28 Jan 2000

[18] Evidence of Patricia Hewitt (Minister for E-commerce) before Trade and Industry Select Committee on 13 Dec 2000, available at <*http://www.parliament.the-stationary-office.co.uk/pa/cm00001/cmselect/emtrdind/66/1121306.htm*>

What becomes clear from the submission is that, apart from the arguments made above, the change in the role of law enforcement agencies from "patrolling preventative" to patrolling investigative" to "directed patrolling, proactive and reactive investigative"[19] was seen to be the main driver for the need for data retention. Data retention, it was argued, was now imperative to enable the agencies to fulfil their new enhanced function; without it, LEAs would be very much deprived of the tools of their trade at a time when a new technology-savvy generation of criminals had emerged.[20]

With an event on the scale of the 9/11 attacks still only a horrible possibility when the report was published, the NCIS' timing seems curious nonetheless. Why was the idea of data retention made a priority issue by LEAs at a time when the use of information technology by organised crime, albeit already a possibility, had not yet fully permeated public consciousness? The answer, as in many other cases, can be found just across the English Channel, in Brussels and Strasbourg.

3.2 Legislative developments in the EU

Regulation 6(2) of the1999 Regulations was based on Art. 6(1) of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector ("Telecommunications Privacy Directive")[21]. Although Art. 14(1) of the same Directive allowed member states to derogate from that obligation and generally to restrict the data subject's right to privacy, this was only possible in very limited circumstances, namely "when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system".

The UK government had not made use of the derogation when implementing the Directive since there was substantial legal doubt about whether a blanket data retention requirement would fall within the provisions of Art. 14(1). What, in its opinion, was required in light of the problems faced by LEAs and other public authorities was a specific enabling provision which clearly stated that the Art. 14(1)

---

[19] NCIS Report, op.sit., para.2.2.1

[20] Notwithstanding any misgivings an active criminal might have about this "changing role" of LEAs, it is without a doubt that any morphing of a reactive force into a proactive, intelligence-based force must be accompanied by stringent safeguards and oversight of that force to avoid the pendulum swinging too far to a place where, far from protecting their citizens' right to presumed innocence, data retention laws lead to a presumption of guilt. As an editorial in The Observer commenting on the report pointed out: "*IT opens up avenues of communication, but it also opens up avenues of government control. The British, with a tradition of an unwritten constitution, executive power and few automatic rights are the most exposed of all. […]" British common law makes no presumption that the individual has the right to privacy and this has generated an extraordinary culture in British officialdom, which presumes a right to investigate. […] We must presume innocence until there is proof of guilt, and the collection of evidence to prove guilt must be at the direction of a court with clear lines of accountability. Instead the NCIS disgracefully recommends that the entire population should be assumed potentially guilty, overturning the first principles of justice on a grand scale. […][The idea] must be killed immediately…*", see The Observer, 3 Dec 2000, "Spied on from cradle to grave – bugging is not the answer to crime"

[21] OJ L 24, 30/1/1998, p. 1

derogations allowed member states to impose on CSPs requirements regarding the wholesale storage of communications data.

In early 2000, in the middle of the 'dot-com boom' when the Internet had become one of the most widely used forms of communication, the EU Commission began to discuss the possibility of "updating" the Telecommunications Privacy Directive to make it more 'technology neutral' and to ensure that "that consumers and users […] get the same level of protection regardless of the technology by which a particular service is delivered"[22]. In July 2000, less than two months before the NCIS submitted its data retention proposals to the Home Office, the EU Commission published a 'Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector' ('E-Privacy Directive') which mirrored almost exactly the existing data protection regime contained in Arts. 6(1) and 14(1) of the Telecommunications Privacy Directive in its Arts. 6(1) and 15(1). A proposal adopted in this form would have closed the door on mandatory data retention for the foreseeable future.

It became clear early on that the LEAs saw what was intended to be a re-enactment of the old Telecommunications Privacy Directive for the digital age as an opportunity to quietly dispose of those provisions contained in the old Directive, which they viewed as the major impediment to their desire for the introduction of a blanket data retention regime. Their lobbying turned out to be successful. The public denial by Patricia Hewitt and Charles Clarke back in the UK notwithstanding, UK representatives in Brussels quietly worked to ensure that the LEAs' demands would be met. During the initial meeting of the Telecommunications Working Party, the body charged with reviewing the proposed Directive to the Committee of Permanent Representatives of the member states to the Council ("COREPER"), the UK delegation[23] entered reservations on the Commission's proposal "requesting that the principle of erasing or rendering the data anonymous be dropped from paragraph 1 [of Art.6]"[24] because they considered "that it did not take into account the needs of law enforcement authorities and did not match the technical requirements of new means of communication via the Internet network and technology"[25].

These reservations were initially rejected not only by the majority of delegations to the Working Party itself but also by the European Parliament in a report prepared by the Committee on Citizens' Freedoms, Rights, Justice and Home Affairs, produced under the direction of rapporteur Marco Cappato. There it was suggested that Art. 6(1) should be adopted more or less unamended, and that any measure taken under Art. 15(1) would have to be "entirely exceptional, based on a specific law which is

---

[22] Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, COM (2000) 385 FINAL, Explanatory Memorandum, para.2

[23] Together with the delegations from France and Belgium.

[24] Report of the Telecommunications Working Party to COREPER of 31 May 2001 on the proposed E-privacy Directive, ECO 147 CODEC 492

[25] Id.

comprehensible to the general public and be authorised by the judicial or competent authorities for individual cases."[26]

However, following the attacks on the World Trade Centre in New York on 11 September 2001, both the European Council and the European Parliament[27] agreed to the UK proposal with the proviso that restrictive measures had to be "appropriate and proportionate within a democratic society" and providing that any restriction had to be a measure of a legislative rather than an executive nature. Just over one year after Patricia Hewitt and Charles Clarke had denied any plans for implementing mandatory data retention, the UK had managed to obtain an enabling provision which would allow member states to do just that.

4. The obligation to introduce mandatory data retention

From the UK's point of view the adoption of the new Directive could not have happened at a more convenient time. Notwithstanding the ongoing negotiations at EU level, the UK government had already introduced the legislative basis for an extensive data retention scheme in the form of the Anti-Terrorism Crime and Security Bill. The bill was introduced on 10 November 2001, less than two months after the terrorist attacks on New York and received Royal Assent on 10 December 2001 after one of the shortest legislative procedures in known history. Section 101 of the Bill allowed the Home Secretary to issue a code of practice, which would in turn permit CSPs to retain communications data "(a) for the purpose of safeguarding national security; or (b) for the purposes of the prevention or detection of crime or the prosecution of offenders" (section 102(5) ATCSA).[28] Compliance with the code of practice was on voluntary basis. However, section 104(1) ATCSA contained a reserve provision, which authorised the Home Secretary to make an order for the mandatory retention of all communications data in the event that the voluntary scheme to be developed under the code of practice proved to be ineffective.

The government's concern in this regard was not entirely unjustified. Having taken legal advice themselves, the CSPs made it clear that they did not consider a voluntary

---

[26] Report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (Hughes Procedure) - Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, A5-0270/2001.

[27] Negotiations were "informed" by a letter sent to President Prodi by US President George Bush on 16 Oct 2001, in which Bush specifically requested, inter alia, to "revise draft privacy directives that call for a mandatory destruction to permit the retention of critical data for a reasonable period", Letter from President Bush to President Prodi of 16 Oct 2001, available from <*http://www.statewatch.org/news/2001/nov/06Ausalet.htm*>

[28] It is outside the scope of this article to describe the reaction to the Bill by civil liberties groups, the communications industry as well as members of both Houses of Parliament. Suffice to say that the provisions contained in Part 11 were severely criticised on the basis that they did not contain any express limit to the scope of the powers of the public authorities authorised under them. There was therefore a risk that they could be used to "secure highly sensitive data for the purpose of investigating very minor offences, or even for monitoring people's communications without any ground for suspecting them of any offence or of threatening national security". For further information see House of Lords, Joint Committee on Human Rights, Second Report Session 2001-02 (14 Nov 2001), para.71; JUSTICE Briefing "Access to communications data by public authorities: The investigatory powers - draft regulation of investigatory powers (Communications data: additional public authorities) Order 2002", p.4; APIG Report, p.11; T Hill, "Data Management: Communications data retention in the UK" (2003) 5, *E-commerce law & policy*, 12

scheme to be sufficient to justify the continued retention of data under the exceptions contained in Part IV of the DPA[29]. They felt that in the event that retention under a voluntary code proved to be unlawful under the DPA and human rights legislation, it would be them, not the government, who would be open to civil claims from affected data subjects[30]. This view was challenged by legal advice obtained by the then Information Commissioner, Elizabeth Frank, in preparation for the expected consultation on the voluntary code. She was assured that "the provisions of ATCS made the retention of data lawful, because Parliament had made their own judgement that it was proportionate to do so for national security reasons"[31]. However, both she and her successor felt that that the use of a voluntary Code of Practice in these circumstances has "severe limitations"[32] and that if data retention was indeed necessary for the specified purposes it would be preferable to introduce a statutory duty as this would provide a greater degree of certainty than was possible under a voluntary scheme.

An order including a voluntary code of practice[33] eventually came into force on 5 December 2003[34] after fierce negotiation with the telecommunications industry and the House of Lords. Much of the criticism focused on the apparent contradiction between the voluntary scheme introduced under ATCSA, which allowed retention solely for the purpose of national security, and access provisions governed by RIPA which permitted an array of government departments to obtain data so retained for any of the – much wider -RIPA purposes, most of which were unconnected to the fight against terrorism. When preparing its report on the ATCS Bill, the Joint Committee on Human Rights of the House of Lords asked the Home Office what legal or technological steps would be taken to ensure that the communications data retained for the purpose of national security would not be available for other purposes. The Home Secretary replied that "the Government [does] not intend to take any legal or technological measures to restrict the use of retained data to national security purposes"[35].

> *"The Government's view is that, if the data are available, they should as a matter of policy be accessible at the request of other*

---

[29] For a detailed analysis of the implications of data retention for the telecommunications industry, see B Zammit, "Traffic Data Retention under EC Law – Implications for the Industry"(2005) 11 *Computer and Telecommunications Law Review*, 1 at 17-22.

[30] Dr. I Walden /E McCormack, "Retaining and accessing communications data" (2003) 8 *Communications Law* 2, 256.

[31] See APIG Report on Communications Data, para. 133

[32] A subject on which they expressed considerable doubt, see the Information Commissioner's response to the Home Office Consultation Paper on a Code of Practice for voluntary retention of communications data, p.1, available at *<http://www.ico.gov.uk/cms/DocumentUploads/Voluntary_Retention_of_Communications_Data_Consultation%20re%E2%80%A6.pdf>*

[33] For a detailed description of the consultation process please see A B Munir and S H M Yasin, "Retention of communications data: A bumpy road ahead" (2004) XXII *The John Marshall Journal of Computer & Information Law* 4.

[34] SI 2003/3175

[35] Second Report of the Joint Committee on Human Rights 2002-03, para.23

> *public authorities for other purposes. […] The Government [does] not accept that the Anti-Terrorism Crime and Security Act 2001, the Human Rights Act 1998 or the ECHR imposes any restriction on the use of retained data for purposes other than protecting national security."*[36]

4.1 The draft Framework Decision v. the draft Data Retention Directive[37]

However, the voluntary code was largely ignored by CSPs. Apart from the legal risks already discussed, this was largely due to the fact that it did not contain provisions dealing with the reimbursement of the costs incurred by CSPs in implementing the scheme. The government, however, made it clear that such costs should be borne by the CSPs as part of the "cost of doing business". Under the circumstances, many CSPs uttered warnings that they might migrate their systems and their data offshore, should the Home Secretary decide to make use of his powers under section 104(1) ATCSA. Apart from the impact such an 'exodus' would have had on the UK economy, such 'offshore-migration' would also have meant that less data would have been available for retention and access by UK public authorities. In the face of such sustained opposition the UK government therefore had to look for alternative ways to achieve its aim. It began to focus on the adoption of a harmonised approach to the issue of data retention by taking steps to convince the other EU member states to introduce minimum data retention periods.

In April 2004, the UK government together with the governments of France, Ireland, and Sweden, submitted a joint proposal for a draft Framework Decision which was intended to put in place a pan-European framework. The proposal required communications service providers to retain, for a minimum of 12 months and a maximum of 36 months, all communications data generated by CSPs within the EU. The alleged aim of the proposal was to assist judicial and law enforcement authorities in investigating terrorism.

In June 2005, the European Parliament released a report in which it criticised the draft Framework Decision on three grounds: the Council's incorrect choice of legal basis, the disproportionality of the measures and the possible contravention of Article 8 of the European Convention on Human Rights. As a result, the European Commission adopted a proposal for a Directive on the retention of telecommunications data on 21 September 2005. It contains similar provisions to the draft Framework Decision proposed by the 4 EU member states, but also included a number of significant differences.

---

[36] Id.

[37] Since the entry into force of the Treaty of Amsterdam, Framework Decisions have replaced joint action as the predominant third pillar instrument. They are used to approximate (align) the laws and regulations of the Member States. Proposals are made on the initiative of the Commission or a Member State and they have to be adopted unanimously. They may be made with the approval of the European Parliament which only needs to be consulted. Framework Decisions are binding on the Member States as to the result to be achieved but leave the choice of form and methods to the national authorities. Directives are made under the first pillar using the co-decision or co-operation procedure. They bind the Member States as to the results to be achieved and they have to be transposed into the national legal framework. Although they leave margin for manoeuvre as to the form and means of implementation, they are usually more prescriptive so that, as a rule, the level of harmonisation between the laws of the Member States is higher.

4.2 The legal basis

The European Parliament's contention that the legal basis for the proposed Framework Decision was flawed was supported by the European Commission as well as the Parliament's Committee on Legal Affairs and the Council's own Legal Service (CLS) in its written opinion of 5 April 2005[38]. While the Council intended to introduce legislation on the basis of Art. 31(1) (c) and 34(2)(b) of the Treaty on the European Union (TEU) as a third pillar measure, the other parties argued that any measure could only be taken on the basis of Art. 95 of the Treaties establishing the European Communities (TEC) ("first pillar") using the co-decision procedure and thereby ensuring full participation of the European Parliament.

Although the Council Presidency (held at the time by the UK) initially ignored the legal advice it received, it eventually acknowledged the CLS's criticism. The reason for this was likely to be the CLS's suggestion that it expected a legal challenge to the Framework Decision to be successful. This could lead to claims for compensation from service providers who would be obliged to implement the measure.

The Presidency will also have been aware of a decision by the European Court of Justice (ECJ) of 13 September 2005[39]. Here the ECJ annulled another Framework Decision (on the protection of the environment through criminal law) on the grounds that the measure, which, in the ECJ's view, should have been adopted under the first pillar, encroached on the powers conferred by the TEC on the Commission and so infringed the TEC.

The issue was debated during a meeting of the Justice and Home Affairs Council (JHA) on 12 October 2005, where a majority of delegations were open to the idea of a directive. However, several continued to favour a Framework Decision and the Council therefore agreed that the Framework Decision would remain on the table while negotiations with the European Parliament continued. This was intended to exert pressure on the Commission and the European Parliament with a view to maximising common ground between the three institutions.

4.3 Data retention provisions contained in the draft Directive

The original draft Directive included a harmonised retention period of 12 months for fixed and mobile telephony data and six months for Internet data. In contrast to the draft Framework Decision, the proposed Directive did not permit individual member states to adopt longer retention periods. While, in the view of the telecommunications industry and civil liberties campaigners, this compared favourably with a maximum retention period of 48 months (contained in the latest version of the draft Framework Decision) it was still held to be unacceptably long given the lack of evidence for the efficiency of any such measure.

---

[38] Opinion of the Council Legal Service of 5 April 2005 on the Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism – Legal basis, Document No 7688/05

[39] *Commission of the European Communities v Council of the European Union*, Case C-176/03, 13 Sept 2005

While the Framework Decision allowed for the retention of data for the purpose of the investigation, detection and prosecution of *any* criminal offence, under the Commission proposal this was restricted to "*serious criminal offences, such as terrorism and organised crime*". However, the Commission proposal included a right to retain data for the purpose of the "*prevention*" of crime, something that had never been considered in the draft Framework Decision and that, it was argued, could well lead to widespread data mining of citizens' travel and communication patterns by law enforcement authorities.

The list of data to be retained under the proposed Directive was similar to the list included in the draft Framework Decision, with the exception of certain Internet data. The proposed Framework Decision required providers to retain data concerning the Internet services used by their subscribers including certain web-browsing data. As pointed out earlier, such data had been seen by many as having the potential to provide law enforcement authorities with an almost complete map of individuals' personal lives, and for that reason it was considered one of the biggest threats to privacy contained in the draft Framework Decision. Under the proposed Directive, such data could not be retained.

The draft Directive did also not include a requirement on providers to retain data relating to unsuccessful call attempts. This measure - which had been inserted in the draft Framework Decision only after its inception at the demand of some of the Council delegations - would have substantially increased the cost of data retention due to the increased storage requirements. The issue had already proved divisive at Council level where some member states feared that such a wide ranging requirement would be rejected by their national courts. The German Constitutional Court, for example, in a decision of 27 July 2005[40] had declared unconstitutional a measure set out in § 33a of the Public Security and Order Act for Lower Saxony which authorised the police force of Lower Saxony to collect personal data through the interception of telephone calls made by persons "where certain facts justify the assumption that they may commit serious criminal offences" in the future. The Court had held that this measure violated individual's' right to the secrecy of their telecommunications (*Art. 10 of the German Constitution*) as it did not comply with the proportionality requirement. The German delegation in the Council argued that any EU measure requiring the retention of data relating to unsuccessful call attempts was bound to fall at the same hurdle.

Finally, the Commission proposal included an obligation on the member states to reimburse service providers for demonstrated additional cost incurred by them in complying with their data retention obligations. The draft Framework Decision did not address the issue of costs apart from a notional statement in a Recital that encouraged member states to consider making appropriate contributions towards the cost incurred by providers. This worried CSPs who feared that many member states would impose the considerable cost of data retention on them. Indeed, as pointed out before, it could possibly be argued that the reluctance of the UK government to pay for data retention was one of the main drivers for its desire for harmonised provisions.

---

[40] German Constitutional Court, Decision of 27 July 2005, 1 BvR 668/04

4.4 Progress of the proposal through the legislative process

The draft Directive was forwarded to the Council and the European Parliament on 23 September 2005 immediately to become the subject of intense political negotiations between the institutions. An agreement reached during the EU's Justice and Home Affairs Council on 12 October 2005 to proceed on the basis of a draft Directive was subject to the condition that any compromise negotiated with the European Parliament would incorporate certain indispensable core elements:

- that the scope of the data to be retained would have to include data on fixed and mobile telephony, Internet access and Internet communication services (telephony and e-mail), as well as data relating to unsuccessful call attempts.
- that the data would have to be retained for a minimum of 6 months for Internet data and 12 months for telephony data with a maximum retention period of 2 years in exceptional circumstances. Member states which had already implemented longer retention periods should be given the possibility to retain such longer periods.
- that there should be discretion for member states in relation to the reimbursement of costs. This should be achieved by having no provision relating to costs in the final Directive.

The Council notified the Commission and the European Parliament that its willingness to proceed on the basis of a Directive was dependent on the institutions reaching agreement before the end of December 2005. In order to meet this deadline the Parliament had to commit to the preparation of a final committee report in less than two months[41]. In addition, Parliament had to adopt the measure using the accelerated "first reading only" procedure. This "undue haste" was criticised by many as an attempt on the part of the Council and, in particular, the UK Presidency, to prevent an in-depth investigation of the actual need for mandatory data retention. More importantly, it sought to ensure that the measure would reach the statute books on the watch of the UK Presidency – before it was due to hand over the reigns to Austria, a declared opponent of data retention, in January 2006. The Council backed its demands with the – in the light of the CLS' Opinion possibly empty - threat that if political agreement could not be reached by the next JHA Council session on 1 December 2005, it reserved its right to proceed on the basis of the draft Framework Decision by scheduling a vote during that session.

While the Council instructed COREPER to finalise an informal agreement on all outstanding issues as soon as possible, the European Parliament appointed Alexander Alvaro MEP as rapporteur for the Committee on Civil Liberties, Justice and Home Affairs ("LIBE") charged with preparing the lead report on the proposed Directive. Alvaro was no newcomer to the subject of data retention, having already prepared Parliament's consultation report on the draft Framework Decision[42]. As a member of the German Liberal Party (FDP), he was a fervent opponent of mandatory data retention and his original report had ultimately led to the rejection of the draft

---

[41] By way of comparison, it took Marco Cappato 14 months to prepare the committee report on the E-privacy Directive.

[42] For a detailed description of the legislative procedure by Alvaro himself see A Alvaro (2006) "Die Richtlinie zur Vorratsdatenspeicherung", *Datenschutz Nachrichten* 2, at 52-55

Framework Decision by the European Parliament. The first draft of his report on the proposed Directive contained no fewer than 238 amendments, incorporating a number of safeguards suggested by the Art. 29 Working Party on data protection issues as well as a reduced retention period of 3 months and a reduced list of data to be retained, removing from the scope of the Directive all Internet data save for data recording the beginning and the termination of each online session.

Alvaro received support in the similarly critical opinions published by the Committee on Industry, Research and Energy (ITRE) under the leadership of rapporteur Angelika Niebler and the Committee on Internal Market and Consumer Protection (IMCO) under Charlotte Cederschiöld, both of whom supported the industry's claim for cost reimbursement. However, he came under intense fire from law enforcement lobbyists and MEPs in favour of data retention.

The report eventually adopted by the LIBE committee during its meeting on 24 November 2005 included a list of compromises, but also proposed a number of important changes to the draft directive:

- Access to and use of retained data should only be permitted for "specified, explicit and legitimate purposes by competent national authorities" and should be subject to judicial approval. Data requested would have to be necessary, relevant and proportional in relation to the purposes for which they are accessed.
- The report rejected the retention of e-mail and voice IP data. It refrained from including data referring to unsuccessful call attempts. Instead it agreed that it should be up to the member states to decide to retain such data.
- Rather than imposing harmonised retention periods the report suggested that it should be up to the member states to decide how long the data should be stored within the timeframe of 6 to 12 months proposed in the original draft. On expiry of the relevant statutory period in each member state the data should be erased.
- Providers should be reimbursed for all "demonstrated additional costs" resulting from implementing the legislation as well as the "demonstrated additional costs of data protection and any future amendments to it" and the "costs arising from making the retained data available to competent national authorities".

While the amendments were discussed in the LIBE committee, the Council instructed COREPER to finalise agreement on all outstanding issues as soon as possible and in any case before the next JHA meeting on 1 December 2005. At the same time the UK Presidency initiated a number of informal "trialogs" with members of the European Parliament in order to achieve a breakthrough.

In a communication to COREPER of 8 November 2005[43] it set out its intention to meet with representatives of the European Parliament on 10 November to discuss amendments to the draft Directive on data retention on the basis of a list of minimum criteria. This list was not only similar to the one previously agreed by the JHS Council

[43] Note from the Presidency to COREPER on Data retention: discussion with the European Parliament, 8 Nov 2005, Inter-institutional file no. 14023/05

on 12 October 2005[44] but also to the draft Framework Decision originally proposed by the UK, Sweden, France and Ireland. However, the right to retain data relating to unsuccessful call attempts had been deleted from the latest Presidency proposal. Its introduction was to be left to the member states as an additional option under Art. 15(1) of the E-Privacy Directive. Member states should also be given the right to determine the retention periods provided that they adopted a minimum period of 6 months and a maximum period of 24 months. Retention of the data for the purpose of the prevention of crime was no longer required. However, this was addressed by the continued application of Article 15(1) of the E-Privacy Directive in relation to data falling outside the scope of the draft Directive and for the retention of data for purposes other than those covered by the draft Directive. Hardest hit were the CSPs by the Presidency's insistence that the question of reimbursement of costs as well as rules on accessing the retained data should be regulated at a national level.

When attempts to achieve an agreement with the LIBE committee along these lines failed, the Presidency targeted the leaders of the two biggest political groups within the EP, the socialist group (PSE) and the conservative group (PPE) directly. Eventually, those leaders, Hans-Gert Poettering (German Christian Democrat) and Martin Schulz (German Social Democrat), in a private meeting with the UK Presidency, agreed to the Council proposal which Charles Clarke, in a press conference on 1 December 2005, presented to the public as a hard won compromise. In fact the "compromise" mirrored exactly the Council's position as set out in the Presidency's communication to COREPER on 8 November. The UK Presidency had not moved an inch while Schulz and Poettering's position had entirely changed, leading to suggestions that the European Parliament had been "sold out" in what many viewed as a demonstration of power mainly led by members of the new German "grand coalition"[45].

The LIBE report as well as the Council compromise were tabled as amendments to the Commission's original draft Directive, and were submitted to the vote of the European Parliament.

Further amendments were tabled by the Greens, who rejected the concept of data retention, and the conservative MEP, Charlotte Cederschiold, who proposed the inclusion of an obligation on member states to reimburse telecommunications providers for the cost of implementing data retention. She justified her amendment on the grounds that providers would otherwise pass on the cost of data retention to their customers which, she considered, would place an unjust burden on EU consumers.

During its plenary session on 14 December, the European Parliament approved the Council compromise in a block vote by 378 votes to 197. The amendment proposed by the Greens was rejected. The Cederschiold amendment was defeated through the acceptance of the Council compromise.

---

[44] see above.

[45] The coalition between Germany's two leading parties, the conservative Christian Democrats (CDU) and the Social Democrats (SPD). It is called the "grand coalition" because it represents a fairly rare departure from the German political custom where one of the two leading parties forms a coalition with one of the smaller parties (i.e. the Greens or the Liberal Democrats (FDP)). Previous grand coalitions have been criticised for creating a situation where there is no effective political opposition.

The Council compromise[46] introduces a retention period of six months to 24 months, with an option for individual member states to introduce longer periods where they face "particular circumstances warranting an extension for a limited period". Retained data will be available for the purpose of the investigation, detection and prosecution of "serious crime". The definition of "serious crime" is left to the national law of the member states.

The list of data to be retained now includes e-mail and internet telephony data. Data relating to unsuccessful call attempts need only be retained if this is already done by a provider for its own business purposes. The draft Directive itself does not include any requirement to this effect.

The Directive does not include any obligation on member states to reimburse service providers for the costs of retention - instead member states are free to decide whether or not they will compensate providers.

Neither does it regulate the gaining of access to, and use of, the retained data by the public and by law enforcement authorities of the member states. This, too, is left for member states to address under their national laws (subject to their international legal obligations), although some MEPs voiced their expectation during the debate in the European Parliament that a certain amount of harmonisation may be the objective of a future Framework Decision under the third pillar.

The draft Directive was approved by the Council on 21 February 2006 and came into force on 3 May 2006. Member states now have 18 months in which to implement the Directive, although they have the option to defer implementation of the provisions requiring the retention of internet data for an additional 18 months.

5. The human rights aspect

The compatibility of the Directive with the right to privacy protected by Article 8 ECHR is at best questionable[47]. According to Lord Lester of Herne Hill and Pannick, this right encompasses the right to be oneself, to live as oneself and to keep to oneself[48]. Warren and Brandeis famously described it as the "right to be left alone."[49] Under Article 8(2) ECHR this right can only be restricted if the restriction is “necessary in a democratic society” for the protection of certain public goods, for instance, to safeguard national security or for the prevention, investigation, detection and prosecution of criminal offences[50]. Any restrictive measure must be appropriate and proportionate. This means that it must balance the interests pursued by it against

---

[46] European Parliament legislative resolution on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD))

[47] For a detailed discussion of the compatibility of blanket data retention with human rights legislation see P Breyer, "Telecommunication data retention and human rights: The compatibility of blanket traffic data retention with the ECHR" (2005) *European Law Journal*, at 365-375

[48] Lord Lester of Herne Hill and D Pannick, (1999) *Human rights: law and practice*, London: Butterworths

[49] S Warren and L D Brandeis, "The right to privacy"(1890) 4, *Harvard law review,* 193.

[50] This requirement is repeated in Recital 4 of the Data Retention directive with reference to Art. 15(1) of the E-Privacy Directive.

its detrimental effects on individuals[51]. The negative impact on civil rights must be proportionate to the aims of the Data Retention Directive.

Questions certainly remain in relation to the effectiveness of data retention. Many commentators have speculated on the ability of LEAs to locate specific data sets, if they form part of data pools of the size which will now be created following the implementation of the Directive. [52] Doubts have also been expressed about the reliability of the retained data, particularly in relation to the ability of law enforcement agencies to prove a suspect's identity[53]. As Caspar Bowden argues:

> *Service providers typically do not handle traffic data logs securely, but even if that were the case, it is important to understand that traffic data cannot prove the identity of the author of an e-mail or the person who actually made a particular call. […] No amount of traffic data by itself can prove an alibi, because while it may be persuasive circumstantially, it does not eliminate the possibility that a bogus trail has been carefully laid by an accomplice.*[54]

Data preservation, the ad hoc "freezing" of communications data, has been suggested as a less invasive alternative to blanket data retention[55], since it affects only a limited number of individuals during specific periods rather than the entire population all of the time. The most important question, however, has rarely been considered by those responsible for introducing the measure. Namely, the effect blanket data retention can

---

[51] B Hofstötter, "The retention of telecommunications data in Europe – A paradigm shift in European data protection law?" (2006) Proceedings of KnowRight 2006, Schriftenreihe der Österreichischen Computer Gesellschaft, Wien

[52] Alexander Alvaro referred to this "wood-for-the-trees" syndrome in his original report: *"If all the traffic data covered by the proposal did indeed have to be stored, the network of a large Internet provider would, even at today's traffic levels, accumulate a data volume of PE 20 - 40 000 terabytes. This is the equivalent of roughly four million kilometres' worth of full files, which, in turn, is equivalent to 10 stacks of files each reaching from Earth to the moon. With a data volume this huge, one search using existing technology, without additional investment, would take 50 to 100 years. The rapid availability of the data required seems, therefore, to be in doubt."*, see draft report of 18 April 2005 on the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications, networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, Committee on Civil Liberties, Justice and Home Affairs, 2004/0813(CNS)

[53] In this context, security expert Bruce Schneier has repeatedly raised the issue of "false positives" and "false negatives", where a false positive is when the system identifies a terrorist plot that really isn't one, a false negative is when the system misses an actual terrorist plot. He argues that even on the most optimistic presumption that a system has a 99% accuracy rate for false positives and a 99.9% accuracy rate for false negatives, and where only 10 data indicators (including phone calls made, purchases, web destinations) had to be searched per US citizen per day, the system would create up to 1 billion false alarms for every real terrorist plot it uncovers, see B Schneier, "Why data mining won't stop terror", *Wired News*, 9 March 2005, available at <*http://www.schneier.com/essay-108.html*>.

[54] Bowden, op. sit., p.6

[55] see for instance "Protecting privacy in the information society", leaflet prepared by the European digital Rights Initiative (EDRI), available at <*http://www.statewatch.org/news/2005/nov/retention-info-nov14.pdf* > last accessed on 16 August 2006. Data preservation is also advocated in Title 2 of the Council of Europe Cybercrime Convention. The Convention is available at <*http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm*>

have on the mind-set of individuals, on their behaviour within society and their relationship with their governments.

Anne Branscombe has said of information that it is the lifeblood that sustains political, social and business decisions. This applies equally to information that personal data such as communications data reveals about us. In a 1983 decision by the German Constitutional Court on the constitutionality of the national census, it was held that the general right to self-determination protected by Art. 2 of the German Constitution included a right to 'informational self-determination'. This term describes the right of an individual to determine when and to whom his personal data are disclosed. The Court confirmed that this right deserved special protection in the light of modern methods of automatic data processing. Personal data which 25 years ago would only have been available in a fragmented way, could, with the help of modern data processing technology, be aggregated and used to built up a revealing picture of an individual. The individual would in most cases be unaware of this and would not be in a position to control and, where necessary, correct the information about him or her and the way in which that information was used. This, the Court argued, had expanded, in a way not previously known, the capability of government officials of inspecting individuals' lives and exerting their authority over them. There was a real risk that the behaviour of individuals could be influenced solely through the application of psychological pressure.

> *A social order, and a legal system which supports it, under which a citizen can no longer be sure who knows what about him, when and on what occasion, is incompatible with the right to informational self-determination. He who is unsure, if information about differing behaviour is at all times noted, permanently stored, used or disclosed as information, will try not to attract attention through such behaviour. Someone who expects, for example, that the participation in an assembly or in a public campaign will be officially registered and that this might put him at risk, will possibly give up the right to exercise the relevant fundamental rights (Art. 8,9 of the German Constitution). This would not only affect an individual's right to develop his personality, but also the common good, as self-determination is an elementary condition for the functioning of a free and democratic society which is based on its citizens' freedom to act and to participate.*[56]

6. Conclusion

The UK Presidency's success in pushing through mandatory data retention in the face of opposition from industry, civil rights organisations and fellow EU member states has to be admired as a master class in diplomacy and political manoeuvring. It cannot be denied that the Directive has been adopted through the most democratic of processes available at EU level. Campaigners lobbying against data retention will be particularly dismayed that a measure which, in their opinion, will be both ineffective and intrusive has been given democratic legitimacy in this way. On the other hand,

---

[56] Decision by the German Constitutional Court on the constitutionality of the national census, 65 BVerfGE 43.

and to put this argument in context, it is likely that the haste with which this proposal was adopted left MEPs little time to consider its effect and to organise effective opposition. It is questionable how many of the MEPs who voted in favour of the Council compromise did so on an informed basis and how many merely followed the voting instructions put forward by their political block.

Civil liberties groups have expressed their concern that some member states may now use their newly created authority to introduce longer data retention periods than those currently set out in the Directive.[57] Such groups will now focus on trying to persuade individual member states to introduce data retention for the minimum of 6 months rather than the maximum of 24 months. They will also argue for the implementation of appropriate safeguards in respect of the storage of, access to and use of retained data by the law enforcement authorities. Some member states may face additional domestic hurdles when trying to implement the Directive at national level. Ireland and Slovakia, meanwhile, are reported to have challenged the legality of the Directive in the European Court of Justice on the basis that it was adopted under the first pillar[58]. They will be encouraged in this endeavour by the ECJ's recent decision in relation to the correct legal basis for the disclosure by EU airlines of passengers' names data to the US Bureau of Customs and Border Protection (CBP)[59].

But until the ECJ makes its decision and while the new legal framework for a comprehensive data retention system is firmly in place, it is time to ask the question who stands to gain from the new regime and who stands to loose? It has been said that protection is not simply needed to guard against unwanted observation, but to guard against the possibility of observation itself. A person who is uncertain whether or not and when they are being watched is likely to behave as if they were being watched constantly.

The German Constitutional Court acknowledged that this permanent threat of being observed is a powerful tool of social control in the hands of the observer - a tool which is open to abuse. The creation of databases which hold substantial amounts of data on the communications of every European citizen is such a tool. Much has been made of the possibility that a lack of security features and safeguards may result in these data falling into the hand of criminals and terrorists. Equally frightening must be the prospect of how such data may be used by government officials within the existing legal framework. Henry Porter observes that:

> *Something enormous and revolutionary is about to happen to us. We are giving the most precious part of ourselves to the government,*

---

[57] Poland, for example, has recently stated that it wishes to introduce retention periods of 15 years although this suggestion was deemed by Charles Clarke during the debate by the European Parliament as "probably falling foul of proportionality requirements", see "Polish plans for 15 years mandatory data retention", EDRI-gram No. 3.24, 5 Dec 2005, available at <*http://www.edri.org/edrigram/number3.24/Poland*>

[58] See Digital Rights Ireland, "Irish government challenges Data Retention Directive – but ignores privacy rights", 7 July 2006, available at <*http://www.digitalrights.ie/2006/07/07/irish-government-challenges-data-retention-directive-but-ignores-privacy-rights/*>

[59] *European Parliament (supported by the European Data Protection Supervisor) v Council of the European Union (supported by Commission of the European Communities and United Kingdom of Great Britain and Northern Ireland) and Commission of the European Communities (supported by United Kingdom of Great Britain and Northern Ireland)*, Cases C-317/04 and C-318/04, 30 May 2006. Unfortunately, the ECJ did not examine if the measure was compliant with Article 8 ECHR.

> *allowing it complete freedom to roam through our privacy. And it's not just to this government, but to the governments of the future, the nature of which we cannot possibly know. And it's not just our privacy - it is the rights and privacy of future generations. While we are comfortable about handing this information over to the state, the citizens of the future may feel strongly about our complacency and our faith in the British government. We have a duty to those people, just as all the people who fought for the rights we enjoy today felt a sense of obligation to us.*[60]

As Edward Bloustein suggested, "privacy guards our individual wants against conformist pressure"[61]. Take away privacy and you create a society of followers. How much do we trust those we are expected to follow?

---

[60] H Porter, "Beware of card tricks", *The Guardian*, 11 July 2006. His remarks were actually made in response to the UK government's plans to introduce ID cards and a national identity register. However, his comments apply equally in relation to data retention.

[61] E Bloustein, "Privacy as an aspect of human dignity: An answer to Dean Prosser" (1964) 39 *New York University Law Review* at 1000-1007.